SST™

Privacy Policy

March 31, 2015

Leveraging Technology to produce Societal Benefits

As technology continues to advance, balancing its benefits against some of its inherent risks to privacy continues to be an issue which confronts us all. What's true for technology in general is also the case in the realm of public safety. Technological advances have provided significant benefits to those tasked with keeping us safe while at the same time raising appropriate dialogue about how we can leverage those benefits while minimizing unwarranted intrusions on personal privacy.

Several police tools and technologies capture information that is already in public view: license plate readers, video cameras at stoplights and ATMs, combined video/audio surveillance cameras, facial recognition algorithms, etc. Unlike general audio and video surveillance devices, such as the tens of thousands of video cameras deployed in our nation's cities which monitor general activities, gunshot detection technology is designed to trigger on loud explosive or impulsive sounds that may likely be gunfire and occur only rarely—and that the public already "hears". Although courts have held that individuals speaking in a manner which can be overheard on public streets do not have the expectation of privacy which would trigger federal wiretapping laws, SST wants to provide stronger protection of individual rights to privacy than is strictly provided for by law. As a result, we developed, and recently strengthened, this privacy policy in order to exceed federal law requirements and to protect individual privacy.

Sensors

Please note: this section refers to the SST ShotSpotter outdoor gunfire detection technology. Indoor sensors are entirely different and provide additional privacy protections and trade-offs.

ShotSpotter sensors are specifically designed to be triggered by loud explosive or "impulsive" sounds only. The entire system is intentionally designed not to permit "live listening" of any sort. Human voices do not trigger ShotSpotter sensors. There are many other loud noises that do not trigger ShotSpotter: car doors slamming, people yelling "bang bang!", loud music, airplane engines, leaf blowers, cheering, highway noise, car engines revving, drag races or tires squealing. ShotSpotter sensors do not use high gain, directional or other specialized microphones.

The discharge of a firearm creates an extremely loud sound (exceeding 150 dB SPL) sound that is detectable up to a mile away. In addition, sensors are intentionally deployed in elevated locations (typically 50-100 feet above street level on building rooftops, sometimes 20-40 feet above ground on a street pole) for three reasons:

1) To maximize their ability to "listen to the horizon" and thereby reduce the number of sensors required;

2) To minimize the background noise from cars and other street noises, thus also reducing the number of sensors required; and

3) To minimize the chance that a human voice will be intelligible, however briefly, in order to protect privacy.

Incident Creation

When a loud explosive noise triggers a sensor, it instantly sends summary data about the acoustic event (e.g. time stamp, sensor location, amplitude and envelope characteristics, etc. but explicitly not the audio of the sound itself) to a centralized processor at our SST-operated data center. There, if no other sensors trigger (i.e., if only one sensor hears the particular impulse), nothing else happens and no incident is created. If multiple sensors (usually 3 or more) report impulsive noises within a narrow time window which are sufficiently loud and mathematically consistent with their having originated at a single location, software algorithms attempt to calculate that origin location. If an accurate location can be determined, the associated sensors' data are aggregated (again, without the audio) and an incident is "created" in a centralized database. A second filter then applies artificial intelligence and statistical techniques to attempt to identify what type of sound originated at this location based on the measurements of the sound. In most cases, the parameters of the sound permit the incident to be filtered out, because it is, e.g., a pile driver or a jackhammer. In a percentage of cases, the characteristics of the sound are consistent with an explosion (gunfire, firework mortar, firecracker, backfire, etc.). In those cases, and only in those cases, the sensors are permitted to push a small snippet of audio to our data center. Otherwise, the audio will be flushed from the sensor's buffer and lost permanently. This is an intentional design: an active step must be taken only in the context of an explosive triggering acoustic event, or the audio is erased and overwritten.

In those cases in which an explosive triggering acoustic event is detected and located, the brief audio snippets are sent to SST's Real Time Incident Review Center (IRC) for analysis and alert qualification by highly trained experts in gunshot acoustics. Within seconds, SST's IRC sends those qualified gunfire alerts directly to a dispatch center, PSAP, patrol officers or other agencies for an effective, coordinated response.

The gunfire alerts that the ShotSpotter system delivers to our police agency clients provide a digital record of violent gun crimes in progress, including minimally brief snippets of audio recordings of those crimes. For any given illegal gunfire incident, that snippet can only contain a few seconds of audio before the first shot and after the last shot. The purpose of these short seconds of audio on either end of the gunshots is to allow a human reviewing in the incident to clearly tell when the shooting starts and stops, including judges and juries during possible future criminal proceedings.

No Live Audio Streaming

As mentioned above, the entire system is intentionally designed not to allow "live listening" of any sort. There is no "listen" button available to law enforcement, or to the staff of our Incident Review Center, except the buttons which replay the specific few seconds of incident audio surrounding an impulse noise determined to likely have originated from an explosive source.

No Private Conversations

ShotSpotter sensors do not have the ability to listen to indoor conversations. They are located in such a fashion to not have the ability to overhear normal speech or conversations on public streets. There has been three extremely rare "edge cases" (3 out of approximately 3**million** incidents detected in the past 10 years), in which a human voice yelling loudly in a public street at the scene of a gunfire incident was overheard for a very brief period (a few seconds) just before or just after a gunshot incident. It would be incorrect factually that ShotSpotter sensors are constantly transmitting audio streams, or somehow have been reconfigured to listen to private conversations. In all cases, the words were yelled loudly, in a public place, at the scene of a gunfire-related crime, and within a few seconds of that event.

Nonetheless, these rare cases caused SST to revisit our privacy policy and further tighten the parameters for audio availability: the permitted audio length is strictly limited to two seconds before and four seconds after. Unless someone is yelling loudly enough to be heard in public, and also doing so within two seconds before or four seconds after a loud, explosive acoustic incident, the audio will be flushed from the sensor's buffer and overwritten. **The simple fact is that there has never been a case of a private conversation overheard or monitored by any ShotSpotter sensor anywhere at any time. Period.**

Policy and Security Minutiae

If you are still with us, here are some additional details:

All servers and software used to process, store and protect data are managed and maintained by SST. Police agencies subscribe to the hosted service on an annual basis, radically streamlining the cost and complexity of using gunfire alert and analysis to enhance awareness, response and community safety. SST owns these data and does not release to anyone other than the customers under contract and according to the terms of that contract, thus further ensuring the safety and security of the data. Customers do not have administrative access to our servers, software, sensors, or any other means to circumvent SST's security and privacy measures.

SST has taken appropriate security approaches to prevent anyone or any entity from gaining unauthorized access to our systems including our processors, networks or sensors. In addition to the fact that the system is designed not to permit live streaming audio, even if an intruder were to take control of our data center and network, they could not "make" a sensor deployed in the field stream audio. It simply isn't possible: the sensors operate on a proprietary protocol and intentionally do not contain code which permits them to stream audio. Asymmetric key encryption is used to control access to sensors, and SST employees are required to use dual-factor authentication to gain access to most critical systems.

In the event that the ShotSpotter system fails to detect an incident, it is SST's policy only to respond to requests for incident data or audio related to specific, verified gunfire incidents. In no event does incident audio extend beyond 2 seconds before and 4 seconds after an incident.

In addition to all of these technical and security measures taken to protect privacy and prevent misuse, SST has adopted a human resources policy to ensure that employees and contractors adhere to our privacy policies.

Summary

In the end, we believe that the privacy of our citizens and the community and social benefits of decreased gun violence are not at odds with each other. Our ultimate goal is to ensure that both are satisfied. We believe we have taken all reasonable and necessary precautions to assure a robust and strong privacy posture. We will continue to review, revise—and strengthen if necessary—these policies.

# # #